

ÖZET

TELEKOMÜNİKASYON UÇBİRİM CİHAZININ BİR GÜVENLİK MODÜLÜNÜN KİŞİSELLEŞTİRİLMESİNE YÖNELİK YÖNTEM

5

Yöntem, bir sunucunun (600) bir güvenlik modülü (300) için bir komut dizisinin alınması ve bir telekomünikasyon uçbirim cihazı vasıtasıyla komut dizisinden bireysel komutların çıkarılması vasıtasıyla komut dizisinin işlenmesini içermektedir. Komutlar, güvenlik modülüne aktarılmaktadır ve güvenlik modülünün komut cevapları alınmaktadır. Güvenlik modülünün komut cevapları sunucuya aktarılmaktadır. Sunucu ve uçbirim cihazı arasındaki iletişim, veriler doğru bir şekilde aktarıldığında sonlandırılmaktadır. Bir güvenlik modülünün kişiselleştirilmesine yönelik bir yöntemin uygulanmasıyla yönelik bir telekomünikasyon uçbirim cihazı için bağlanmış bir istem dahil edilmektedir.

10

İSTEMLER

1. Bir telekomünikasyon uç birimi cihazı(200) içindeki bir güvenlik modülünün (300) kişiselleştirilmesine yönelik yöntem olup telekomünikasyon uç birimin cihazında aşağıdaki adımlar **ile karakterize edilmektedir:**

- güvenlik modülü (300) için bir sunucudan (600) bir komut dizisinin alınması
- komut dizisinin aşağıdakiler vasıtasıyla işlenmesi

telekomünikasyon uçbirim cihazı(200) tarafından bireysel komutların komut dizisinden çıkarılması ve komutların güvenlik modülüne (300) aktarılması

burada güvenlik modülü (300), kişiselleştirme öncesinde şebeke işletmecisinde (700) kimlik doğrulama için kullanılmamaktadır ve

- komut dizisi, kullanılarak şebeke işletmecisine özel kişiselleştirme verilerini aktarmaktadır burada
- komut dizisinin telekomünikasyon uçbirim cihazı(200) içinde işlenmesi sırasında güvenlik modülünün (300) komut cevapları alınmaktadır ve
- kişiselleştirme yöntemi, güvenlik modülünün (300) son komut cevabını sunucuya (600) göndererek tamamlanmaktadır

2. Telekomünikasyon uçbirim cihazı (200), bir kişiselleştirme modunda olması **ile karakterize edilen**, İstem 1'e göre yöntem.

3. Sunucunun (600), güvenlik modülüne (300) aktarılması gereken verileri komut dizisi olarak düzenlemesi **ile karakterize edilen**, İstem 1 veya 2'ye göre yöntem.

4. İstem 1 ila 3'e göre yöntem olup, sunucunun (600) aktarılan komut cevapları değerlendirilmesi ile; ve aşağıdakiler **ile karakterize edilmektedir**

- tüm verilerin doğru bir şekilde aktarıldığı ve aktarılacak başka verilerin bulunmadığı durumlarda telekomünikasyon uçbirim cihazıyla (200) iletişimin sonlandırılması veya
- son komut dizisinin aktarılması sırasında telafi edilemez bir hata oluşması halinde telekomünikasyon uçbirim cihazıyla (200) iletişimin sonlandırılması veya

- son komut dizisinin aktarılmasında telafi edilebilir bir hata oluşması halinde (i) alt adımla başlayarak aynı komut dizisini yeniden göndermesi, veya
- son komut dizisinin doğru bir şekilde aktarılmı ve aktarılacak başka verilerin de bulunduğu durumlarda (i) alt adımla başlayarak ilave bir komut sekansını göndermesi.

5

5. Komut dizisinin, bir blok olarak telekomünikasyon uçbirim cihazına (200) aktarılmasında sunucunun (600, 400) tüm bloğun aktarılma doğruluğunun kontrolü için telekomünikasyon uçbirim cihazının (200) sekansın son komutuna bir cevapla yeterli olması **ile karakterize edilen**, İstem 4'e göre yöntem.

10

6. Komutların güvenlik modülüne aktarılma, bireysel komutlar ardışık iletimi dolayısıyla etkilenmesi, burada bireysel komutların aktarılma doğruluk kontrolünün, güvenlik modülünün (300) her bir bireysel komuta verdiği bir cevaba bağlanarak etkilenmesi **ile**, ve aktarılacak başka komutun bulunmadığı veya bir aktarımın doğru bir şekilde yapılmadığı durumlarda komut aktarılma durdurulması **ile karakterize edilen**, İstem 4 veya 5'e göre yöntem.

15

7. Telekomünikasyon uçbirim cihazı (200) olarak JavaCard ile entegre J2ME-etkin bir uçbirim cihazının kullanılması **ile karakterize edilen**, İstemler 1 ila 6'dan birine göre yöntem.

20

8. Sunucunun (600, 400) güvenlik modülüyle (300) iletişiminin, özellikle MIDlet şeklinde uçbirim cihazı üzerinde kurulan birim (900) aracılığıyla gerçekleşmesi **ile karakterize edilen**, İstemler 1 ila 7'den birine göre yöntem.

25

9. Uçbirim cihazların (200) bir yandan sunucuya (400, 600) olan bağlantı ve öte yandan güvenlik modülüne (300) olan bağlantı bağimsiz uygulama parçacıkları içerisinde gerçekleşmesi **ile karakterize edilen**, İstemler 1 ila 8'den birine göre yöntem.

30

10. Komut dizisinin XML olarak kodlanması **ile karakterize edilen**, İstemler 1 ila 9'dan birine göre yöntem.

35

11. Telekomünikasyon uçbirim cihazları (200) bir cep telefonu veya bir PDA (Kişisel Sayısal Yardımcı) olması ile karakterize edilen, İstemler 1 ila 10'dan birine göre yöntem.

12. Komut dizisinin, her bir komut için güvenlik modülünün komuta beklenen cevapları içermesi ile karakterize edilen, İstemler 1 ila 11'den birine göre yöntem.

13. Önceki istemlerden birine göre yöntem olup, aşağıdakiler ile karakterize edilmektedir

- güvenlik modülünün telekomünikasyon uçbirim cihazları (200) takılması (3); ve
- en az bir komut dizisi yardımıyla kişiselleştirilmesi (4).

14. Bir kullanıcı fazından (7, 9) önce bir birinci ISD-anahtarları (ISD, verici güvenlik alanı) hizmet sağlayıcıları özel bir ISD-anahtarları için değiştirilmesi (5) ile karakterize edilen, önceki istemlerden birine göre yöntem.

15. Bir kullanıcı fazından (7, 9) önce en az bir yeni uygulamanın, özellikle bir NFC-uygulamasının, güvenlik modülüne girilmesi, uygulama sağlayıcıları (701, 711, 721) için güvenlik modülü (301) üzerinde kendine ait alanların rezerve edilmesi ve her birinin kendine ait anahtarla donatılması ile karakterize edilen, önceki istemlerden birine göre yöntem.

16. İstemler 1 ila 15'den birine göre bir yöntemin uygulanması için uyarlanan bir telekomünikasyon uçbirim cihazı

TARİFNAME

TELEKOMÜNİKASYON UÇBİRİM CİHAZININ BİR GÜVENLİK MODÜLÜNÜN KİŞİSELLEŞTİRİLMESİNE YÖNELİK YÖNTEM

5

Buluş, bir telekomünikasyon uçbirim cihazı içindeki güvenlik modülünün kişiselleştirilmesi ile ilgilidir. Telekomünikasyon uçbirim cihazları olarak, GSM, UMTS, CDMA veya benzer şebekeler üzerinden bir PLMN (public land mobile network) içinde iletişim kuran tüm cihazlar, yani özellikle mobil telefonlar, kişisel sayısal yardımcılar (PDA'lar) ve benzerleri kastedilmektedir.

10

Bu yapılandırma bağlamında örneğin telekomünikasyon uçbirim cihazları mobil şebekeye karşı kimliğinin tespiti veya kullanılarak telekomünikasyon uçbirimi cihazına karşı kimliğinin tespiti, bir güvenlik işlevi olarak kabul edilmektedir. Bu tür güvenlik işlevleri, telekomünikasyon uçbirim cihazında bulunan güvenlik modülleri üzerinde gerçekleştirilmektedir; genelde SIM-kartlar üzerinde. Son olarak bu tür güvenlik modüllerini, genişletilmiş birer TMP (trusted platform module = donanımsal şifreleme kartı) olarak yer alması önerilmiştir. TPM'ler, geleneksel SIM-kartlardan farklı olarak, telekomünikasyon uçbirim cihazına sabit olarak entegre olmaktadır.

15

20

Bir telekomünikasyon uçbirim cihazının bir mobil şebekeye bağlanabilmesi ve mobil şebeke işletmecisinin güvenlik merkezi nezdinde kimliğinin tespit edilebilmesi için, telekomünikasyon uçbirim cihazının güvenlik modülünün gerekli verilerle donatılması gerekmektedir; özellikle ilgili şebeke işletmecisinin gerekli gizli kimlik doğrulama algoritmaları ve uygun kodlarıyla. Güvenlik modülünün bu gerekli, şebeke işletmecisine özel verilerle donatılması mevcut buluş bağlamında kişiselleştirme olarak adlandırılmaktadır. Verilerin kendisi, devamında şebeke işletmecisine özel veriler olarak adlandırılmaktadır.

25

30

Bugüne kadar çoğunlukla hâlihazırda bu şebeke işletmecisine özel verilerle donatılmış olan güvenlik modülleri müşterilere teslim edilmektedir. Bu, mobil telefon cihazları için SIM-kartlar için geçerlidir. Sabit bir şekilde telekomünikasyon uçbirim cihazına entegre güvenlik modüllerinin olumsuz yanı sıra güvenlik modülünün üretimi sırasında bile ve onun telekomünikasyon uçbirim cihazına takılmasından önce şebeke işletmecisinin biliniyor olması gerektiğidir veya farklı şebeke işletmecileri için farklı güvenlik modülleri üretilmesi gerektiğidir; bu ise birbirinin aynı güvenlik modüllerinin uygun masraflı ve tekdüzen olarak üretilmesine olanak vermemektedir.

35

EP 1 002 440 B1 sayılı Patent Dokümanı GSM-çiplerinin müşteriler tarafından bir telsiz arayüzü üzerinden kişiselleştirilmesi için bir yöntem açıklamaktadır. Şebeke işletmecisi tarafından önceden kişiselleştirilmiş bir çip, kullanılarak ilk defa kullanılarak şebekesine bağlandığında, otomatik olarak tam kişiselleştirilmektedir. Tam kişiselleştirmede 5 telekomünikasyon uçbirim cihazı ile şebeke işletmecisinin güvenlik merkezi arasında bir bağlantı kurulduktan sonra yeni, ikinci bir gizli kod, güvenlik merkeziyle hazırlanmaktadır ve akabinde güvenlik modülüne dâhil etmek üzere telekomünikasyon uçbirim cihazına iletilmektedir. Güvenlik modülünün telekomünikasyon uçbirim cihazına dâhil edildiği sırada şebeke işletmecisine özel veriler ihtiva etmesi gerektiği şeklindeki olumsuzluk, yine 10 sürmektedir.

EP 0 956 730 B1 sayılı Patent Dokümanı telsiz arayüz üzerinden geçici bir kullanıcılığının verilmesi için bir yöntem açıklamaktadır. Bu kullanıcı kimliği, sadece özel bir bağlantı kurulumu için istenmektedir ve kullanılmaktadır. Telekomünikasyon uçbirim cihazı kalıcı 15 olarak kişiselleştirilmemektedir.

US 2004/0246071 A1 sayılı Patent Dokümanı uygulama kodları bir sunucudan uçbirim cihazındaki SIM-kartına, SIM-kart içinde deşifre olan bir SMS ile iletilmesini açıklamaktadır.

EP 1 276 339 A1 sayılı Patent Dokümanı bir sunucudan bir programı bir SIM-kartına yüklenmesi için bir yöntemle ilgili olup kullanılarak listeden bir program seçmektedir ve sunucu, SIM-kartın bir özellik listesine göre bir şifreleme metodu seçmektedir. 20

Buluşun amacı bir telekomünikasyon uçbirim cihazında sabit olarak yer alan ve henüz şebeke 25 işletmecisine özel veriler içermeyen bir güvenlik modülünün etkili ve güvenli bir şekilde kişiselleştirilmesi için önerilerde bulunmaktır.

Bu amaç, ilgili istemlerin özelliklerine sahip bir yöntem ile yerine getirilmektedir. Buna bağlı olarak istemlerde buluşa ait yararlı yapılar ve geliştirmeler yer almaktadır. 30

Buluşa göre bir telekomünikasyon uçbirim cihazındaki bir güvenlik modülünün şebeke işletmecisine ait verilerle kişiselleştirilmesi için telekomünikasyon uçbirim cihazı üzerinde aşağıdaki işlemler yapılmaktadır.

35 - Güvenlik modülü için bir sunucudan bir komut dizisi alınmaktadır.

- Komut dizisinin aşağıdakiler vasıtasıyla işlenmesi

Komut dizisindeki belirli komutların telekomünikasyon uçbirim cihazı tarafından elde edilmesi,

- 5 Komutlar güvenlik modülüne gönderilmesi ve güvenlik modülünün komut cevaplarını alması ve

- Güvenlik modülünün son komut cevaplarını sunucuya aktarılması

- 10 Sözleşme akdinden sonra şebeke işletmecisi tarafından kullanıya iletilen, kişiselleştirme için gerekli kimlik doğrulama bilgileri, kullanıcılarda öncelik telekomünikasyon uçbirim cihazında bulunabilmektedir ve kullanıcı tarafından telekomünikasyon uçbirim cihazının güvenlik modülüne geçirilebilmektedir. Bu kimlik doğrulama bilgileri, çeşitli şekillerde kullanıcılarda bulunabilmektedir ve çeşitli şekillerde telekomünikasyon uçbirim cihazının güvenlik modülüne uygulanabilmektedir; örneğin alfa nümerik rakam dizisi manüel şekilde girilerek, RFID-Tag okutularak, bilgiler bluetooth veya WLAN-arayüzü üzerinden aktararak, barkot taratarak, akustik bilgilerin fotoğraflanarak akabinde OCR uygulamasıyla dönüştürülerek ve benzeri.

- 20 Buluş, tekdüzen güvenlik modülleri üretilmesine ve telekomünikasyon uçbirim cihazlarına uygulanmasına olanak vermektedir. Daha sonra abonesi olunacak özel şebeke işletmecisinin önceden bilinmesine gerek bulunmamaktadır, zira güncel teknik standartlara göre bir ön kişiselleştirme yapılmamaktadır. Kimlik doğrulama bilgileri, telekomünikasyon uçbirim cihazı tarafından algılandıktan sonra telekomünikasyon uçbirim cihazı tarafından doğrudan ve herhangi bir manüel işlem gerektirmeksizin kişiselleştirme için kullanılabilmektedir. Güncel 25 mobil şebekelerin değiştirilmesi, gerekli olmamaktadır. Aynı şekilde aynı güvenlik modülüyle şebeke işletmecisinin değiştirilmesi de mümkün olmaktadır.

- Kişiselleştirme yöntemi, telekomünikasyon uçbirim cihazının bir güvenlik merkezine bağlantı kurmasıyla devam etmektedir. Güvenlik merkeziyle ilk bağlantının kurulması için gerekli 30 bilgiler, örneğin sadece bir defalıkla güvenlik merkezine bağlanmak için kullanılan, ancak hiçbir şekilde kişiselleştirme yoluyla ihtiyaçlarına göre telekomünikasyon uçbirim cihazının uyarılacağı özel şebeke işletmecisine bir bağlantı olmayan, sanal şebeke işletmecisinin (MVNO) kodları ve algoritmaları gibi tekdüzen şekilde tüm güvenlik modüllerinde bulunabilmektedir veya kullanıcı tarafından kimlik doğrulama bilgileriyle birlikte güvenlik 35 modülüne aktarılabilir.

Kişiselleştirme yönteminin bir sonraki adımında kimlik doğrulama bilgileri, güvenlik merkezine aktarılmaktadır. Kimlik doğrulama bilgileri, sözleşme akdinden sonra şebeke işletmecisinin örneğin bilgi ve hesap kesim amaçları için kimliğini tespit edebilmek için, bilgisine ulaştırılarak uygulama verilerini (subscription data) kapsamaktadır. Bunun dışında kimlik doğrulama bilgileri, örneğin şebeke işletmecisi, güvenlik merkezi, erişim modu vs. gibi daha başka bilgiler de içerebilmektedir. Bu kimlik doğrulama bilgileri, bu bilgilerin güvenlik modülüne girişinden ve güvenlik merkeziyle bağlantı kurulmasından sonra kullanılarak kişiselleştirme yöntemini otomatik olarak başka herhangi bir önlem alınmaksızın devam ettirmesi için gerekli tüm bilgileri içermektedir.

Güvenlik merkezi, alınan kimlik doğrulama bilgilerinin doğruluğunu değerlendirilmektedir ve olumlu sonuç alınması durumunda telekomünikasyon uçbirim cihazına güvenli bir bağlantı kurmaktadır. Bunun dışında güvenlik merkezi, kimlik doğrulama bilgileri üzerinden kullanılarak hangi şebeke işletmecisine özel kişiselleştirme bilgilerine ihtiyaç olduğunu tespit edebilmektedir ve bu bilgilerin telekomünikasyon uçbirim cihazına güvenlik modülüne aktarılmasını başlatmaktadır. Yani tam otomatik bir kişiselleştirme gerçekleşmektedir. Kullanıcıya duruma göre yöntemin işleyişi hakkında örneğin bir ekran üzerinden bilgilendirilebilmektedir.

Telekomünikasyon uçbirim cihazına kimlik doğrulama bilgileri uygulanmadan önce özel bir moda geçirilmesi tercih edilmektedir. Bu şekilde kişiselleştirme yöntemi kolaylaştırılmaktadır çünkü bu özel mod durumunda başka işlevler aktif olmamaktadır ve bu sayede kişiselleştirme, otomatik olarak işleyebilmektedir. Bunun dışında bu mod, güvenli bir iletişim sağlanacağı olacak şekilde ayarlanabilmektedir. Bu özel mod, mevcut buluş bağlamında kişiselleştirme modu olarak adlandırılmaktadır.

Kişiselleştirme bilgilerinin aktarılmasından sonra telekomünikasyon uçbirim cihazı normal çalışma moduna getirilerek olağan iletişim amaçları için kullanılabilir. Telekomünikasyon uçbirim cihazına kullanıcının değiştirmesi durumunda, örneğin satış yapılarak, ödünç verilerek veya hediye dilerek, veya kullanıcının şebeke işletmecisini değiştirmesi durumunda, açılan kişiselleştirme yöntemi, kişiselleştirme modunda yeniden başlatılabilmektedir. Şahven kullanılması veya suistimali önlemek amacıyla bir şifre konulabilmektedir.

Sonrasında buluşteki şekiller vasıtasıyla örnekler bazında açıklanmaktadır. Buna göre:

Şekil 1 buluşa göre bir kişiselleştirme yöntemi için uygun bir sistemi,

Şekil 2 XML kodlu bir komut dizisini,

5 Şekil 3 MIDlet içinde bir yöntemi işleyişini,

Şekil 4 bir güvenlik modülü, bir MIDlet ve bir sunucu arasındaki iletişim yöntemini,

Şekil 5 bir MIDlet ve bir sunucu arasındaki iletişim yöntemini,

10

Şekil 6 güvenlik modüllerinin telsiz arayüzü üzerinden yönetilmesi için bir sistemin mimarisini ve

Şekil 7 bir güvenlik modülünün yaşam döngüsünün gösterimini göstermektedir.

15

Buluşa göre bir kişiselleştirme yönteminin tercih edilen bir yapılandırma örneği, devamında tek tek adımlara ayrılmış bir şekilde daha detaylı olarak gösterilmektedir. Şekil 1, kişiselleştirme yönteminin uygulanmasında yarayan bir sistemi detaylarıyla göstermektedir. Bu sistem, kimlik doğrulama bilgilerini (100), dışarıda kimlik doğrulama bilgilerinin (100) bulunduğ ve bir güvenlik modülüne (300) sahip olan bir telekomünikasyon uçbirim cihazı (200), bir veri bankası (500) ve bir sunucu (600) kapsayan bir kişiselleştiricinin (1000) bir güvenlik merkezini (400), bir veya daha fazla şebeke işletmecisi (700, 710, 720) ve bir mobil telsiz şebekeyi (800) kapsamaktadır. Kişiselleştirme yöntemi tek tek adımlar halinde aşağıda detaylı olarak açıklanmaktadır.

25

1. Telekomünikasyon uçbirim cihazı (200), kişiselleştirme yöntemi için kişiselleştirme modunda bulunmaktadır veya bu moda geçirilmektedir. Kişiselleştirme için gerekli olan, telekomünikasyon uçbirim cihazı (200) dışarıda bulunan kimlik doğrulama bilgileri (100) yukarıda açıklanan şekillerden biri uygulanarak cihaza (200) girilmektedir; örneğin alfa nümerik rakam dizisi manuel şekilde girilerek, RFID-Tag okutularak, bilgiler bluetooth veya WLAN-arayüzü üzerinden aktararak, barkot taratarak, akustik bilgilerin fotoğraflanarak akabinde OCR uygulamasıyla dönüştürülerek ve benzeri. (WO 2006/006001 A1 sayılı Patent Dokümanı) benzer şekildeki mobil telsiz cihazı (200) dışarıda yoğunlaştırılmış bilgileri uygun okuma teknikleriyle bir mobil telsiz cihazına girilmesi, orada açılması ve böylece örneğin bir takvim kayd gibi özel bir aksiyonu otomatik

30

35

olarak başlatılmasın için izole bir fikir açılmaktadır)

2. Akabinde kullanıcının telekomünikasyon uçbirim cihazından (200) mobil telsiz şebekesine (800) bağlantı kurmayarak başlatacağı. Bu, örneğin sadece bir defalık olarak güvenlik merkezine (400) bağlanmak için kullanılan, ancak hiçbir şekilde kişiselleştirme yoluyla ihtiyaçlarına göre telekomünikasyon uçbirim cihazından (200) uyarlanacağı özel şebeke işletmecisine (700, 710, 720) bir bağlantı olmayan bir sanal şebeke işletmecisinin, tüm güvenlik modüllerinde (300) tekdüzen şekilde bulunabilen kodlar ve algoritmalar yardımıyla yapılabilmektedir. Tercih olarak bu kodlar ve kimlik doğrulama algoritmaları da ilk olarak kullanıcının tarafından telekomünikasyon uçbirim cihazına (200) girilmektedir; örneğin telekomünikasyon uçbirim cihazından (200) mümkün olduğunca evrensel bir kullanıcının mümkün olduğu için kimlik doğrulama bilgileriyle (100) eşzamanlı olarak. Bu adıma kurulan bağlantı şebeke altyapısının tarafından sadece kişiselleştiricinin (1000) güvenlik merkezi (400) ile güvenli modülü (300) arasında bilgi alışverişi olabilecek şekilde ayarlanmıştır.

3. Kimlik doğrulama bilgileri (100), mobil telsiz şebeke (800) üzerinden kişiselleştiricinin (1000) güvenlik merkezine (400) gönderilmektedir. Bu, kullanıcının tarafından başlatılarak olabilmektedir veya otomatik olarak güvenlik modülü (300) tarafından başlatılabilmektedir.

4. Güvenlik merkezi (400), veri bankasına (500) başvurarak, alınan kimlik doğrulama bilgileri (100) için hangi muhtemel şebeke işletmecilerinin (operatör) (700, 710, 720) mevcut olduğunu tespit etmektedir.

5. Muhtemel şebeke işletmecileri (700, 710, 720) hakkındaki bilgiler, uygun bir bilgi hizmeti (örneğin GPRS, SMS) yardımıyla telekomünikasyon uçbirim cihazına gönderilmektedir. Bu bilgi, kullanıcının örneğin bir ekran üzerinden verilebilmektedir.

6. Kullanıcı şimdi istediği şebeke işletmecisini (700) seçmektedir. Bu seçim, avantajlı bir şekilde SIM-ayar kiti komutlarıyla yapılabilmektedir. Bu şekilde şebeke işletmecisinin (700, 710, 720) seçimiyle ilgili bilgi, güvenlik modülüne (300), örneğin bir SIM-kartına, doğrudan aktarılmaktadır.

7. Güvenlik modülü (300), kullanıcının seçimini mobil telsiz şebekesi (800) üzerinden kişiselleştiricinin (1000) güvenlik merkezine (400) göndermektedir. Bu, iletişimi güvenli bir şekilde sağlamak için, opsiyonel olarak şifreli ve / veya kriptolu olarak yapılabilmektedir. (4 numaralı adımda sadece bir muhtemel şebeke işletmecisi varsa, 5 ila 7. adımlara gerek kalmamaktadır)

8. Şimdi güvenlik merkezinde (400) ilgili kişiselleştirme bilgileri, özellikle kimlik doğrulama algoritması ve buna ait kodlar gibi şebeke işletmecisine özel bilgiler, fakat

ek uygulamalar için muhtemelen program kodları da öyle, bir veri bankasından (500) alınmaktadır

9. Kişiselleştirme bilgileri, güvenlik modülüne (300) gönderilmektedir. Bu, iletişimi güvenli bir şekilde sağlamak için, opsiyonel olarak şifreli ve / veya kriptolu olarak yapılabilmektedir.

10. Güvenlik modülünde (300) alınan bilgilerin doğruluğu kontrol edilir ve olumlu sonuç alınması durumunda uygun bir yerde güvenlik modülüne (300) entegre edilmektedir.

11. Son adımda hatasız olarak tamamlanmış olması durumunda güvenlik merkezi (400), bununla ilgili güvenlik modülünden (300) bir ileti almaktadır. Böylece güvenlik modül (300), yeni bir şebeke işletmecisi (700) için kişiselleştirilmiş olmaktadır ve şebeke işletmecisi (700) tarafından açıldığı andan itibaren normal çalışmaya geçebilmektedir.

12. Güvenlik merkezinin (400) güvenlik modülünden (300) aldığı kişiselleştirme bilgilerinin başarılı transferiyle ilgili bilgiler, şebeke işletmecisine (700) iletilmektedir. Bu bilgiler, büyük ölçüde günümüzde "response-bilgiler" olarak kişiselleştiriciler tarafından şebeke işletmecilerine iletilen bilgilere eşittir. Bu bilgilerin doğru girişinden sonra şebeke işletmecisi (700), güvenlik modülünü (300) açacaktır, böylece ilgili telekomünikasyon uçbirim cihazı (200) normal moda geri döndürülebilmektedir ve olağan iletişim amaçları için kullanılabilmektedir.

Devamında güvenlik merkezi (400) ile telekomünikasyon uçbirim cihazı (200) güvenlik modülü (300) arasında bilgi aktarımı teknik olarak gerçekleştirilmesi için tercih edilen bir olarak açıklanmakla özellikle önceki 9, 10 ve 11 numaralı adımlar ele alınmaktadır

Tercih olarak telekomünikasyon uçbirim cihazı (200) olarak, J2ME-etkin ve JavaCard 2.x ve 2.2.1 küresel platform standartlarında entegre güvenlik modülü (300) olan bir cep telefonu kullanılmaktadır. Güvenlik modülünde (300), öncelikle Java Applets ve küresel platform güvenlik alanları bulunmamaktadır. Verici güvenlik alanı (Issuer Security Domain) kodları (ENC, KEK, MAC), çipe uygun veya bir Master-Key-Setine uygun olabilen ilk kodlar olmaktadır. Bu durumda güvenlik modülü (300), hiçbir uygulama için kullanılamamaktadır, özellikle de bir şebeke işletmecisinde (700) kimlik doğrulama için uygun olmamaktadır

Şekiller 2 ila 5'e göre şimdi bir mobil telefonun (200) güvenlik modülü (300) ile kişiselleştiricinin (1000) güvenlik merkezinin (400) sunucusu (600) arasındaki iletişim yöntemi açıklanmaktadır

Tercihen güvenlik modülü (300) ile sunucu (600) arasındaki iletişim için APDU-Protokolü (application protocol data units) kullanılmaktadır. Burada bilgiler, blok halinde aktarılmakta olup bir bilgi bloğu, daima ya bir komuttan ya da bir komut cevabından oluşmaktadır. Burada güvenlik modülü genelde pasif (slave) rolü üstlenmektedir ve sunucu (master) tarafından gönderilen, cevaplayacağı komutları beklemektedir. Bilgi bloklarının özel yapısı, her bilgi bloğunda istenen bilgilerin aktarılması için alan (data field) bırakılmaktadır. Yani sunucudan (600) güvenlik modülüne (300) gönderilecek olan bilgiler, APDU-komutlara paketlenmektedir. Bu tür komutlardan oluşan bir dizi, bir komut dizisine birleştirilmektedir. Şekil 2, örnek olarak XML (Extensible Markup Language) dilinde kodlanmış bir komut dizisini göstermektedir.

Şekiller 3 ve 4'te güvenlik modülü (300) ile sunucu (600) arasındaki iletişim, şema halinde gösterilmektedir. Cep telefonunda (200), bir uygulama programlama arayüzü (API) (application programming interface) üzerinden cep telefonunun (200) güvenlik modülüne (300) erişim sağlayan ve sunucuyla (600) iletişim kurabilen bir MIDlet (900) bulunmaktadır (J2ME, MIDP2.0 spesifikasyonlarına göre).

Bu iletişim kurma işlemi, sunucunun bir arayüzü (600a), bir servlet üzerinden gerçekleşmektedir. Şekil 3, Servlet (600a) üzerinden Midlet (900) ve sunucu (600) arasındaki iletişimi göstermektedir. MIDlet (900) tarafından ilk iletişim kurulduktan sonra Servlet (600a), sunucuda (600) ilk komut dizisini alarak onu örneğin XML dilinde kodlar, MIDlet (900)'e gönderir. Şekil 4'de MIDlet (900) tarafından bu komando sekansının devamında nasıl işlem görüldüğü gösterilmektedir. Bireysel komutlar, ardından MIDlet (900) tarafından, her seferinde bir cevap ile bir önce almış olduğu komuta cevap veren güvenlik modülüne (300) gönderilmektedir. Tüm komutlar, örneğin n-komutları işlendikten sonra MIDlet (900), güvenlik modülünün (300) n-te-komutuna olan cevabını, Servlet (600a) üzerinden sunucuya (600) göndermektedir. Şimdi ise yöntem, yukarıda açıklandığı şekliyle, güvenlik modülünün (300) n-te-komutuna olan cevabına bağlı olarak ve aktarılacak olan bilgilerin ve bunla birlikte aktarılacak olan komut sekanslarının yoğunluğuna bağlı olarak, Şekiller 3 ve 4'de gösterildiği gibi, defalarca tekrarlanabilmektedir.

Sonrasında Şekil 5'e göre MIDlet (900) içindeki yöntem daha yakından gösterilmektedir. Bir uygulama programlama arayüzü (API) üzerinden güvenlik modülüne (300) bir bağlantı kurmuş olan MIDlet (900), kişiselleştirme işlemini başlatmak için, kişiselleştiricinin (1000) sunucusuna (600) örneğin bir https-bağlantısı üzerinden bir kanal açmaktadır. Sunucu (600),

- başvurunun geçerliliğini kontrol etmektedir ve olumlu sonuçlanmasında güvenlik modülü (300) için olan bilgileri, bir komut dizisi şeklinde hazırlamaktadır. Bu komut dizisi, örneğin https-başvurusu için cevap olarak MIDlet (900)'e gönderilmektedir. Şimdi komut dizisi MIDlet (300) tarafından işlem görmektedir; burada komut sekansından bireysel
- 5 komutlar çıkarılarak ardışık olarak, yukarıda açıklandığı şekliyle bu tür bir komuta cevap verecek olan güvenlik modülüne (300) gönderilmektedir. Güvenlik modülü (300) tarafından beklentiye uygun cevap gelmesi durumunda sekanstaki sonraki komut, güvenlik modülüne (300) gönderilmektedir. Verilen cevabın beklentiye uygun olmaması durumunda, MIDlet (900) tarafından komut dizisi aktarıldıktan sonra ve güvenlik modülünden (300)
- 10 alınan en son cevap, komut sayaç durumuyla birlikte kişiselleştiricinin (1000) sunucusuna (600) geri gönderilmektedir. Sekansın tüm komutlarının başarıyla işlenmiş olması durumunda, MIDlet tarafından güvenlik modülünden (300) alınan en son cevap, komut sayaç durumuyla birlikte sunucuya gönderilmektedir.
- 15 Sunucunun (600), gönderilen bilgilerin güvenlik modülüne (300) doğru aktarıldığının kontrol edebilmesi için, sadece güvenlik modülünün (300) son komuta vermiş olduğu cevaba ve MIDlet (900) tarafından güvenlik modülüne (300) kaç tane komutun aktarıldığını, yeni bir komut dizisini işleme almadan önce öğrendikten sonra her işlemten sonra 1 artırılarak tespit eden komut sayacı durumuna ihtiyaç bulunmaktadır. Böylece komut sekanslarının
- 20 sunucudan (600) güvenlik modülüne (300) aktarılmasındaki işlemi, bireysel komutların aktarılmasına nazaran iletişim hacminden tasarruf etmektedir ve bilgi aktarımında daha hızlı ve daha etkili bir hale getirmektedir; çünkü sunucu (600), güvenlik modülünün (300) her komuta vereceği cevapı beklemek durumunda değildir ve her cevabı, sunucuya aktarılmasında zorunlu değildir.
- 25 Komut dizisi, örneğin XML dilinde kodlanılabilmektedir (bakınız Şekil 2). Alternatif olarak başka formatlar da düşünülebilmektedir; örneğin virgülle ayrılmış komutlar ve benzeri. Şekil 2'de örnek olarak gösterilen komut dizisinde "ExpectedResponse" hanesi, her birinde "90 00" ile doldurulmuş olmaktadır. Bu hane "90 00" opsiyoneldir; çünkü bu, doğru şekilde yerine
- 30 getirilen bir komutta JavaCard'ın verdiği standart cevaptır ve bu cevapta komut dizisinin başarılı bir şekilde işlem görmeye devam edeceğinin garanti edildiği, varsayılmaktadır. Böylece bu Standard-Expected-Response bilgisinin de aktarılmasında gerek olmamakla ek aktarım hacminden de tasarruf edilmektedir.
- 35 Hem komut dizisinin tamamen doğru olarak işlenmesinde hem güvenlik modülünün (300)

5 beklenmedik cevaplar nedeniyle kesintide güvenlik modülünün (300) cevapları MIDlet (900) üzerinden kişiselleştiricinin (1000) sunucusuna (600) iletilmesinden sonra onun tarafından yeniden bir komut dizisi gönderilebilmektedir ve yöntem, yukarıda açıklandığı gibi baştan başlamaktadır. Bunun olmadığı durumlarda MIDlet (900) tarafından sunucuyla (600) olan iletişim sonlandırılmaktadır ve gerektiğinde kullanıldığı bir statü bildiriminde bulunmaktadır.

MIDlet ve kişiselleştiricinin (1000) sunucusu (600) arasındaki bağlantı bir yandan ve cep telefonunun (200) güvenlik modülüne (300) olan bağlantı öte yandan, çeşitli uygulama parçaları arasında yer alabilmektedir.

10

Yukarıda açıklandığı gibi telekomünikasyon uçbirim cihazlarındaki güvenlik modüllerinin kişiselleştirilmesindekine benzer, güvenlik modülleri hizmet sağlayıcılarındaki çeşitli yapılandırmalar için de olabilmektedir; örneğin NFC-uygulamalar için. Near Field Communication (Yakın alan iletişimi) (NFC), bilgilerin 13,56 MHz frekans alanındaki manyetik alanlarda kısa bir mesafe (yaklaşık 20 cm) üzerinden temassız olarak aktarılmasına yarayan bir teknoloji olarak tanınlanmaktadır ve cihazlara, hem temassız kart olarak hem kart okuyucu olarak işlev görme olanağı sunmaktadır. Günümüzde saniyede 424KB seviyelerinde veri aktarımı mümkün olabilmektedir. Güvenlik konusunda hassas uygulama alanlarında bu teknolojinin geniş kapsamlı olarak kullanılmasına engel olan, NFC-standardının kendisinin herhangi bir güvenlik önlemi öngörmüyor olmasıdır. Örneğin gömülü güvenlik denetleyicisi, SIM-Kart, Güvenlik-Flaş-Kart ve benzeri gibi güvenlik modülleri bulunan standart NFC-cihazlarla kombinasyonda güvenli NFC-işlemi, çok sayıda uygulamayı gerçekleştirme olanağı sunmaktadır; örneğin ödeme işlevi, erişim kontrolü, dijital hak yönetimi (DRM), kimlik kontrolü, içerik indirme, biletlendirme, cihaz yapılandırması ve benzeri. Bir telekomünikasyon uçbirim cihazının güvenlik modülü içerisinde birbirinden bağımsız olarak birden fazla NFC-uygulamaları yüklemek ve kullanmak mümkün olmaktadır.

25

Sonrasında Şekiller 6 ve 7'ye göre OTA-Secure-Chip-Management-System olarak adlandırılan, NFC etkin telekomünikasyon uçbirim cihazlarındaki güvenlik modüllerinin bir telsiz arayüzü (OTA, Over The Air) üzerinden yönetilmesine yarayan bir sistem açılmaktadır. Tüm sisteminin tarifi için, Şekil 6, bir güvenlik modülünün on faza bölünmüş yaşam döngüsünü göstermektedir. Güvenlik modülü üretildikten sonra (Faz 1), ilk ISD-anahtarının (ISD, verici güvenlik alanı) güvenlik modülüne girildiği ve kendisine net bir kimlik (ID) verildiği Faz 2'de kişiselleştirme gerçekleşmektedir. Faz 3'te, güvenlik modülü bir uçbirim cihazına monte edilmektedir. Yukarıda açıklandığı gibi, şebeke işletmecisindeki kişiselleştirme, Faz 5'te, yani

30

35

aktivasyon fazında yeni uygulamalar, özellikle NFC-uygulamalar, güvenlik modülüne girmek üzere hazırlanmaktadır. Faz 4'te gerçekleşmektedir. Faz 6'da ilgili uygulama yazılımı güvenlik modülünde yüklenmektedir ve Faz 7 kullanımı fazı olarak başlamadan önce, kullanıcılara göre uyarlanmaktadır. Faz 8'de uygulamaların muhtemel uyarlamaları gerçekleşmektedir veya Faz 9'da, yani bir başka kullanım fazında uygulanacak olan yeni uygulamalar yüklenmektedir (Fazlar 8 ve 9 arasındaki değişim, birçok kez yapılabilir). Faz 10'da, güvenlik modülünün yaşam döngüsü sona ermektedir.

OTA-Secure-Chip-Management-System'in kullanıldığı Fazlar 5, 6 ve 8, devamında daha ayrıntılı olarak açıklanmaktadır. Bir hizmet sağlayıcısı (1001) ile bir telekomünikasyon uçbirim cihazı (201) güvenlik modülü (301) arasındaki veri aktarım teknik işlemi, tercih olarak yukarıda da Şekiller 3 ila 5'teki tercih edilen yapılandırma örnekleri bazında tarif edilmiş olduğu gibi gerçekleşmektedir.

Şekil 7'de tüm sistem mimarisi gösterilmekte olup içerisinde bir hizmet sağlayıcısı (1001) bir güvenlik merkezinde (401) bulunan bir kart uygulama yönetim sunucusunun (CAMS) (601), bir NFC-modülü (250) kapsayan NFC-etkin bir telekomünikasyon uçbirim cihazı (201) güvenlik modülüyle (301) güvenlik modülünü bir veya daha fazla uygulama sağlayıcısı (701, 711, 721) uygulamalar için ayarlanması için doğrudan iletişim kurması öngörülmektedir. Bu iletişim, sadece telsiz arayüzü üzerinden bir mobil telsiz şebekesi (800) üzerinden yapılmaktadır. Kullanıcıda telekomünikasyon uçbirim cihazı dışında mevcut olan kimlik bilgileri (101) yukarıda açıklanan şekillerden biriyle kişiselleştirme fazında (Faz 4) telekomünikasyon uçbirim cihazı (201) girildikten sonra, güvenlik modülü (301), Faz 5'te aktif hale getirtilebilmektedir.

Aktivasyon (Faz 5)

Bu adımda güvenlik modülü (301), bir veya birden fazla spesifik uygulamanın gereksinimlerine göre hazırlanmaktadır. Faz 2'de güvenlik modülüne (301) girilmiş olan ISD-anahtar (ISD, verici güvenlik alanı) bir telsiz arayüzü üzerinden hizmet sağlayıcıya özel ISD-anahtarla değiştirilmektedir. Böylece güvenlik modülü (301), hizmet sağlayıcısı (1001) tarafından gönderilen bilgilerin kabul edildiğini ve yüklenmesine izin verildiği anlamaktadır. Aynı kod, hizmet sağlayıcısı (1001) bir cihaz yönetim veri bankasında (501) da kaydedilmektedir.

Yeni uygulama sağlayıcı alanlarının yüklenmesi (Faz 6'da)

Bu adında kullanılarak tarafından seçilmiş olan her bir uygulama sağlayıcısı (701, 711, 721) için, SSD (supplementary security domains) olarak adlandırılan özel alanlar, güvenlik modülü (301) üzerinde rezerve edilmektedir ve her biri kendine özel bir SSD-anahtarla donatılmaktadır bunlar yine aynı şekilde hizmet sağlayıcısı (1001) Device-Management-veri bankasında (501) kaydedilmektedir. Bu alanlar, ilgili uygulamaların dışarıdan erişime karşı güvenli bir şekilde kaydedildiği ve uygulanabildiği "güvenli konteynörler" olarak kabul edilmektedir. Birden fazla uygulama sağlayıcılar (701, 711, 721), kendilerine ait tamamlayıcı güvenlik alanları (SSD) birbirinden bağımsız ve rahatsızlık vermeden yan yana çalıştırılabilen, aynı güvenlik modülü (301) zerine yükleyebilmektedirler. Aynı şekilde bu adı da bir telsiz arayüzü üzerinden gerçekleştirilmektedir.

Uygulama indirme (Faz 6'da)

Her uygulama sağlayıcısı (701, 711, 721) güvenlik modülünde (301) kendine ait alan tahsis edildikten sonra, uygulama yazılımını indirme işlemi başlatılabilmektedir. Bu işlem, bir telsiz arayüzü üzerinden ve ilgili SSD-anahtarla güvenli şekilde gerçekleştirilmektedir. İndirme işlemi, Trusted Third Party (Güvenilir Üçüncü Taraf) (TTP) olarak da adlandırılan ve güvenlik modülünün (301) yönetimini burada açıldığında gibi yerine getiren, hizmet sağlayıcısı (1001) tarafından da başlatılabildiği gibi bizzat uygulama sağlayıcısı (701, 711, 721) tarafından da başlatılabilmektedir.

Uygulamanın kişiselleştirilmesi (Faz 6'da)

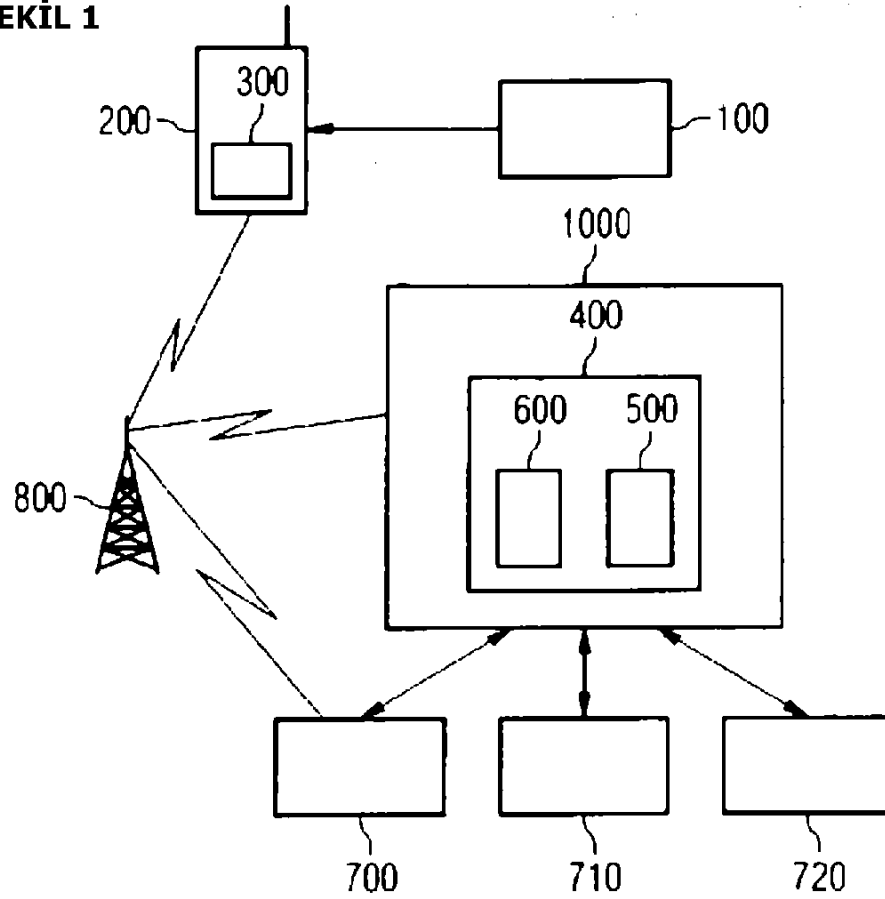
Bu adımda, yapılandırılmaya göre uyarlanmış olan kullanıcı bilgileri, ilgili SSD-anahtarla kodlanarak güvenlik modülüne (301) aktarılacak suretiyle ilgili uygulama, kullanıcıya göre ayarlanmaktadır Aynı şekilde yine bu adı, hem TTR (1001) tarafından hem uygulama sağlayıcısı (701, 711, 721) tarafından yapılabilmektedir ve bir telsiz arayüzü üzerinden gerçekleştirilmektedir.

Uyarlama ve yeni uygulamalar (Faz 8)

Çalışma süresi içerisinde güvenlik modülünün (301), uygulama sağlayıcıları (701, 711, 721) yeni bilgilerine göre uyarlanması gerekmektedir ve duruma göre yeni uygulamalar da içerebilmektedir. Aynı şekilde bu uyarlama da TTP (1001) tarafından veya uygulama sağlayıcısı (701, 711, 721) tarafından başlatılabilmektedir ve bir telsiz arayüzü üzerinden

gerçekleşmektedir.

ŞEKİL 1



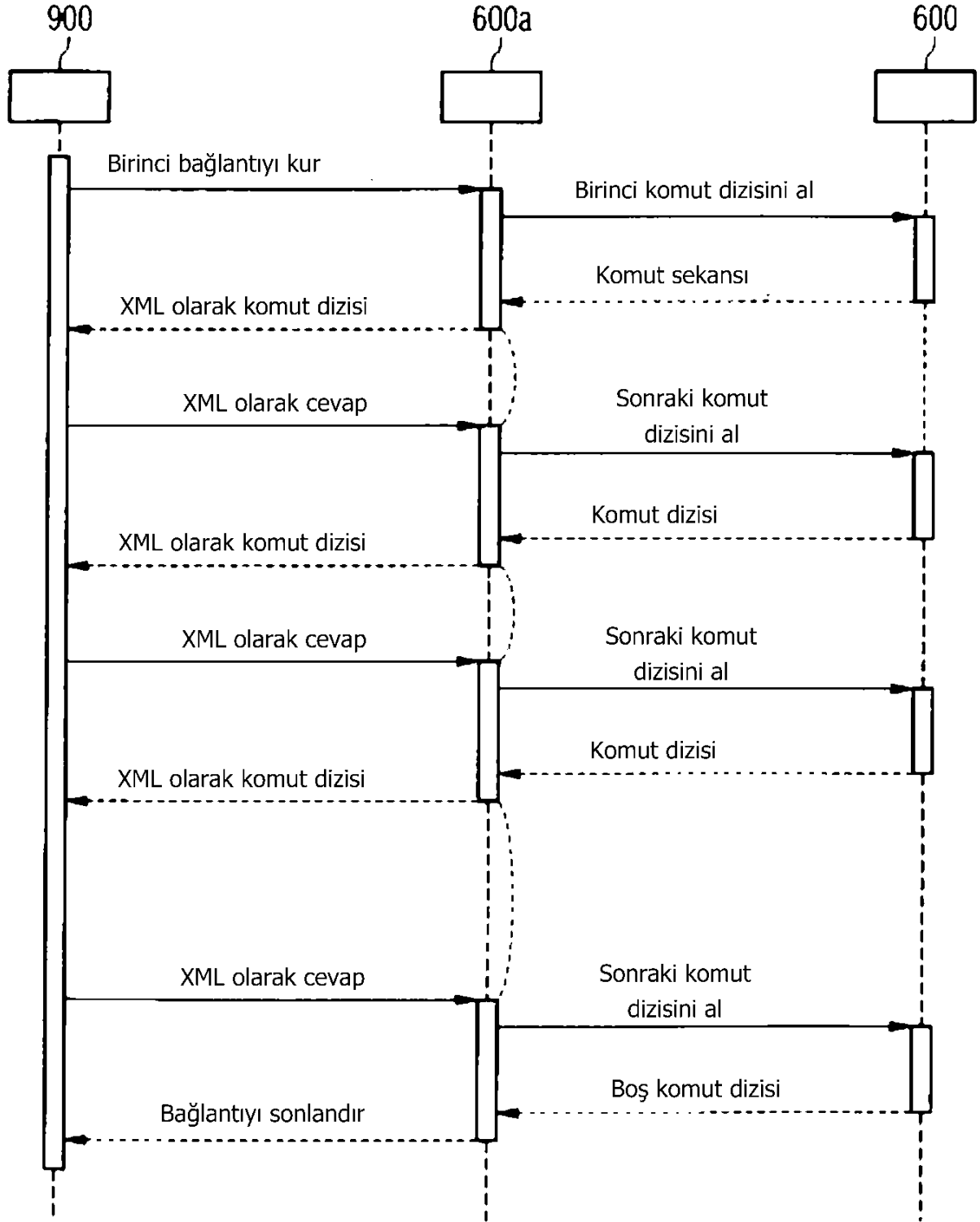
ŞEKİL 2

```

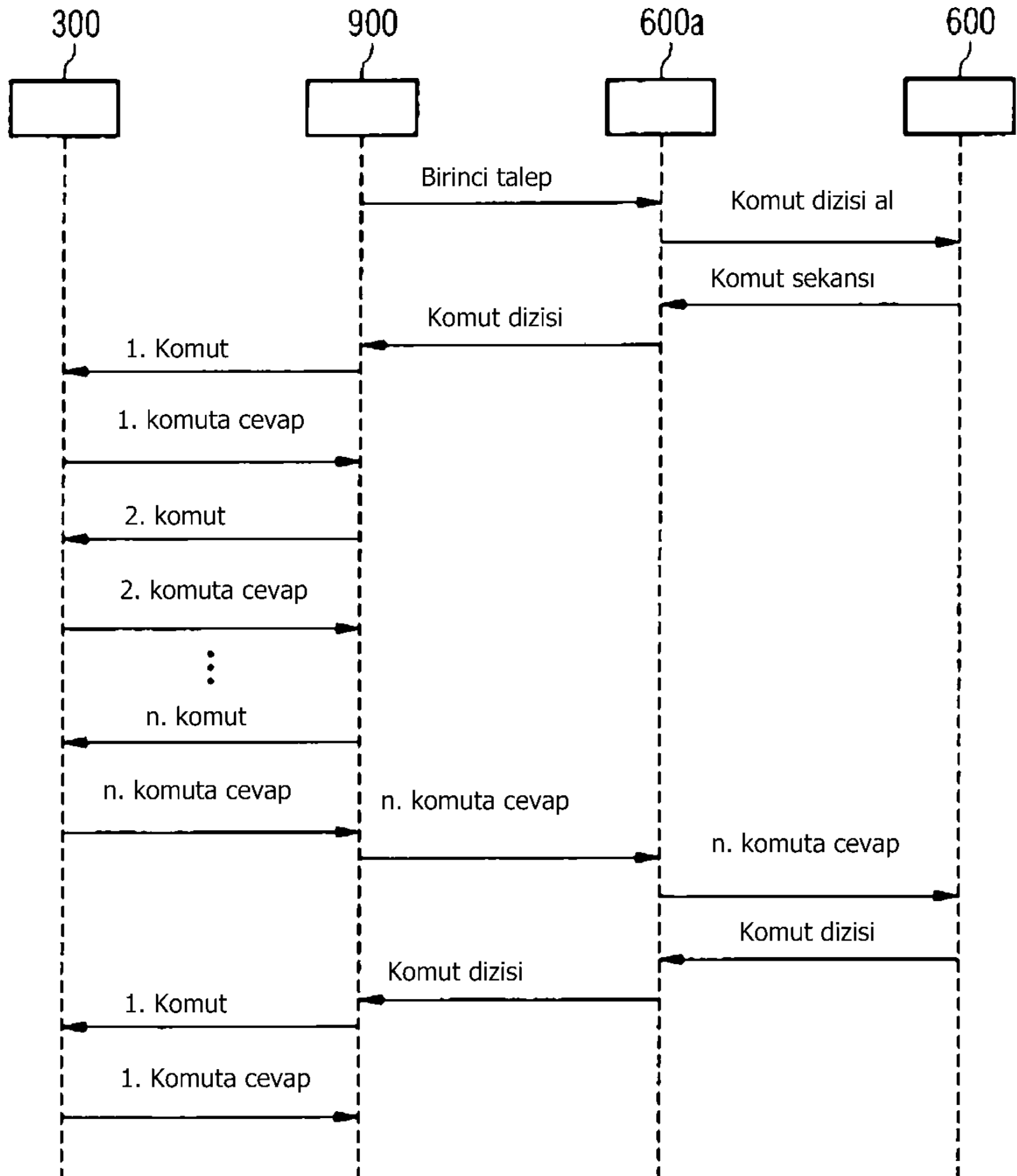
-<APDUList> -<APDU>
  <ID>1</ID>
  <Value>00 A4 00 0C 02 3F 00</Value>
  <ExpectedResponse>9000</ExpectedResponse>
</APDU>
-<APDU>
  <ID>2</ID>
  <Value>00 84 00 00 00</Value>
  <ExpectedResponse > 90 00 </ExpectedResponse >
</APDU>
-<APDU>
  <ID>3</ID>
  <Value>80 F6 00 00 00</Value>
  <ExpectedResponse > 90 00 </ExpectedResponse >
</APDU>
</APDUList>

```

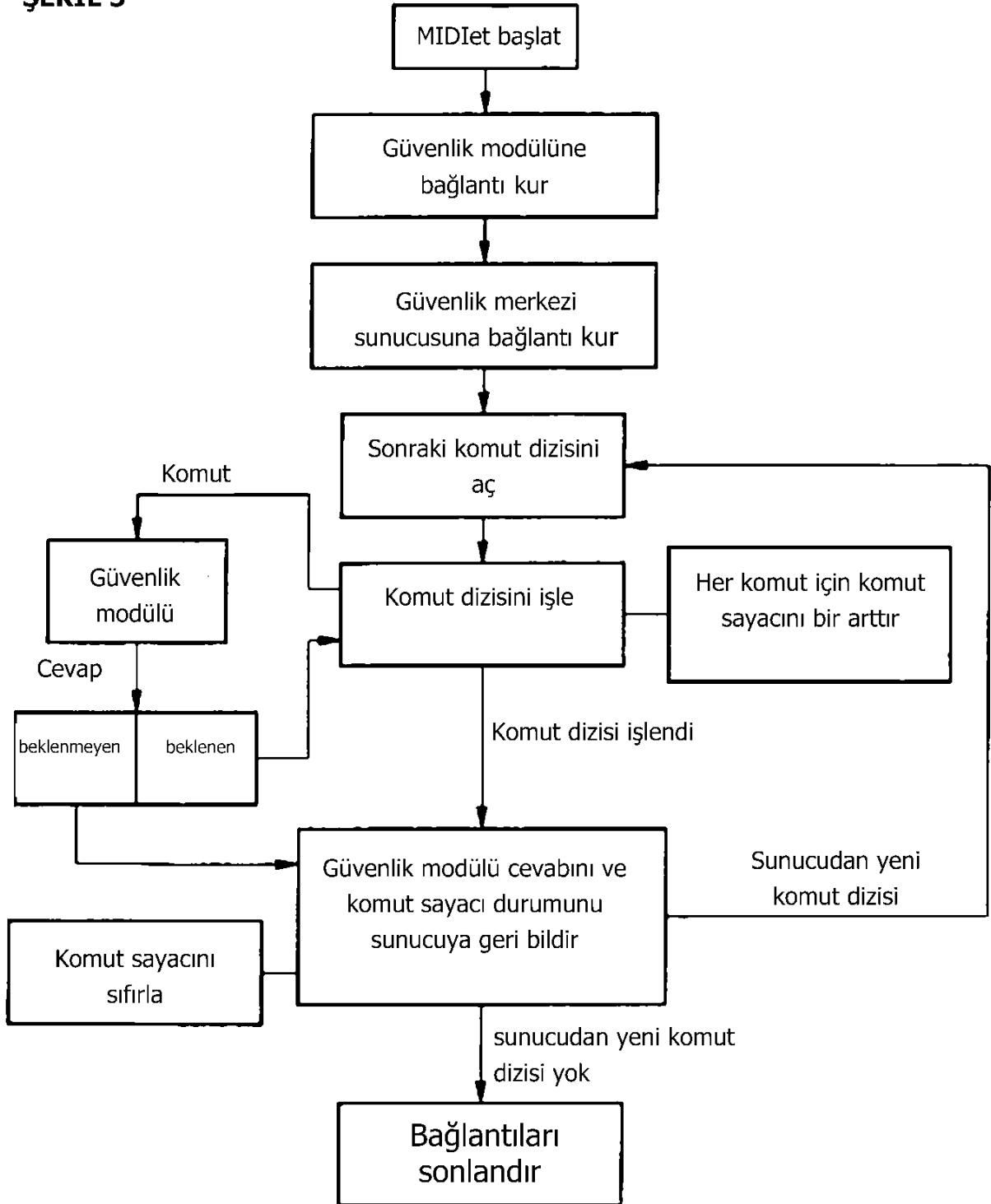
ŞEKİL 3



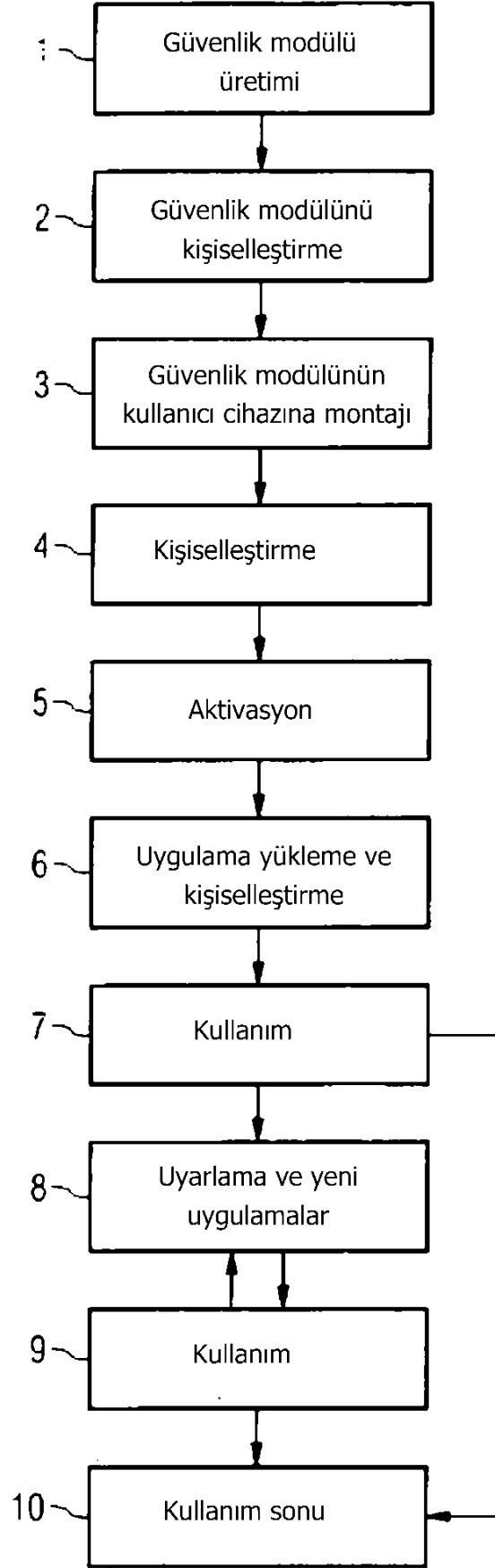
ŞEKİL 4



ŞEKİL 5



ŞEKİL 6



ŞEKİL 7

